

ABSTRACT

METHOD FOR TESTING AN INTEGRATED CIRCUIT
INCLUDING HARDWARE AND/OR SOFTWARE
PARTS HAVING A CONFIDENTIAL NATURE

This method uses a tester (T) capable of being connected to an integrated circuit (CI) to be tested.

A random number (RNG-C) is generated and ciphered using a key (k) by a cipher algorithm to obtain a password ($G_K(\text{RNG})\text{-C}$). The random number (RNG-C) is
5 sent to the tester (T) in which the received random number (RNG-C) is ciphered using the same key (k) by a same cipher algorithm to generate therein a second password ($G_K(\text{RNG})\text{-T}$). This latter is sent to the integrated circuit (CI) to be compared to the first password ($G_K(\text{RNG})\text{-C}$). The test of the confidential parts (1) of the circuit is only authorised if the two passwords exhibit the required match.

10

Figure 1